CCC:CMM
F.#2019R00050

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ APR 12 2019 ★
LONG ISLAND OFFICE

IN THE MATTER OF THE SEARCH OF ONE BLACK AVVIO CELLULAR TELEPHONE ("SUBJECT DEVICE"); WHICH IS CURRENTLY LOCATED IN THE EASTERN DISTRICT OF NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. MJ - 19 342

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Brian O'Keefe, being first duly sworn, hereby depose and state as follows:[1]

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device—which device is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent with the Drug Enforcement Administration ("DEA") for approximately 20 years and am currently assigned to the DEA New York Division, Long Island District Office. I have been involved in the investigation of numerous

[1] Because the purpose of this affidavit is to set forth only those facts necessary to establish probable cause for a search warrant, I have not described all the relevant facts and circumstances of which I am aware.

cases involving the trafficking of narcotics. In the course of those investigations, I have conducted physical surveillance, debriefed cooperating witnesses and confidential informants, and interviewed civilian witnesses. I have participated in investigations involving search warrants, including searches of electronic devices, and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to communicate with one another and to conceal their activities from detection by law enforcement authorities.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code Sections 841 and 846 have been committed (the "Target Offenses"). There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is one black Avvio cellular telephone (the "SUBJECT DEVICE"). The SUBJECT DEVICE is currently located in the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On or about January 15, 2019, Joseph Gabriel Bermudez-Matos ("Bermudez-Matos") arrived at MacArthur Airport in Long Island, New York aboard Southwest Airlines flight 803 from Baltimore, Maryland, to Islip, New York, having begun his travel aboard Southwest Airlines flight 627 in San Juan, Puerto Rico.

8. At MacArthur Airport, as part of an enforcement operation, two DEA special agents ("Officer 1" and "Officer 2") approached Bermudez-Matos for participation in a consensual interview while Bermudez-Matos was walking within the baggage claim area. Bermudez-Matos had one checked blue-colored roller suitcase (the "Suitcase") and one blue-colored "Sketchers" knapsack. The handle of the Suitcase was in Bermudez-Matos's hand, and Bermudez-Matos was walking with the Suitcase, when Officers 1 and 2 approached Bermudez-Matos. Officer 1 identified Officers 1 and 2 as DEA Special Agents. Officer 1 asked Bermudez-Matos, in sum and substance, whether he owned the Suitcase. Bermudez-Matos said "no, no," immediately dropped the Suitcase, and ran in the direction of two automatic exit doors leading outside of MacArthur Airport.

9. Officers 1 and 2 pursued Bermudez-Matos. When the automatic exit doors did not immediately open, Bermudez-Matos turned and continued running within the airport. As he continued running, he flung a large, cylindrical-shaped trashcan into Officer 1, causing

Officer 1 to fall and fracture three bones in his shoulder. Officer 2, as well as certain officers with the Suffolk County Police Department, apprehended Bermudez-Matos.

10. Bermudez-Matos was then taken to a law enforcement room within MacArthur Airport. He was subsequently taken to a smaller examination room within MacArthur Airport, where he was informed of his right to an attorney. At that time, Bermudez-Matos provided DEA officers with verbal consent to search the Suitcase, which he acknowledged belonged to him

11. Prior to the provision of verbal consent by Bermudez-Matos to search the Suitcase, a Certified Narcotics Detection Canine Handler (the "Handler") exposed the Suitcase to "Dodge," his trained canine, for Dodge to inspect the exterior of the Suitcase. In response to being exposed to the exterior of the Suitcase, Dodge reacted to the Suitcase, which, based on the information obtained from the Handler, indicated a positive alert that the Suitcase contained a controlled substance or the residue of a controlled substance.

12. Subsequent to the Handler's inspection of the Suitcase and the verbal consent by Bermudez-Matos, DEA officers searched the suitcase. That search revealed the presence of eight large bricks of a white powdery substance. The white powdery substance from the Suitcase field-tested positive for cocaine. A total gross weight of the eight bricks recovered from the Suitcase, including their packaging, was approximately 10.5 kilograms.

13. On February 14, 2019, a grand jury sitting in the Eastern District of New York returned a multi-count indictment charging Bermudez-Matos with conspiracy to distribute and possess with intent to distribute cocaine, in violation of Title 21, United States Code, Sections 846 and 841(b)(1)(A)(ii)(II), possession with intent to distribute cocaine, in

violation of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(A)(ii)(II), and assault on a federal officer, in violation of Title 21, United States Code, Sections 111(a)(1) and 111(b).

14. At the time of his January 15, 2019 arrest, Bermudez-Matos was in possession of the SUBJECT DEVICE. Law enforcement officers took custody of the device at that time.

15. Based on the above, there is probable cause to believe that Bermudez-Matos, as well as others whose identities are unknown at this time, were involved in the distribution and possession with intent to distribute a controlled substance. Further, there is probable cause to believe that information on the SUBJECT DEVICE will produce evidence probative of the crimes under investigation.

16. Based on my training and experience, I know that individuals who engage in drug trafficking commonly use mobile devices such as cellular telephones to communicate with co-conspirators through voice calls, text messages, emails, and other means. I further know that individuals who commit such drug trafficking crimes often use mobile devices to arrange and plan the execution of the crimes.

17. The SUBJECT DEVICE is currently in the lawful possession of the DEA after being recovered from Bermudez-Matos incident to his lawful arrest.

18. The SUBJECT DEVICE is currently located in the Eastern District of New York. I know that the SUBJECT DEVICE has been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of the DEA.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite

repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities that allows it to serve as wireless telephones, digital cameras, portable media players, PDAs, and GPS navigation devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICE.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT

DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICE already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Brian O'Keefe
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me
on April 12, 2019:

/S/ STEVEN I. LOCKE

HONORABLE STEVEN I. LOCKE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is one black Avvio cellular telephone (the "SUBJECT DEVICE"). The SUBJECT DEVICE is currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846 and involve Bermudez-Matos and his co-conspirators, including:

   a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;

   b. lists of customers and related identifying information;

   c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   e. any information recording Bermudez-Matos's schedule or travel;

   f. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the SUBJECT DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as

evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the times the SUBECT DEVICE was used;

5. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE; and

6. Contextual information necessary to understand the evidence described in this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.